EXHIBIT 7

REVIEW

Network Forensic Tools

Elementary, My Dear Watson

We tested a range of investigative tools, from full-featured remote image acquisition products to specialized apps that can dig deep into text or mail stores. Find out which ones will make you into an IT Super Sleuth!

Dec 9, 2004 - By Marisa Mack

In This Article

Hundreds of tools and applications address forensic incident response, but there's no single solution. The scope is too broad: A complete forensic incident-response toolkit must incorporate data acquisition, text and file searching, Internet history analysis, and proprietary analysis of mail files and data stores. That's a tall order.

Still, many incident response and forensics applications claim to meet it. To test these promises, we asked 12 vendors to participate in a comparative review in our Chicago Neohapsis Real-World Labs®. AccessData, dtSearch, Guidance Software, Paraben and Technology Pathways sent a variety of products, and we added the open-source Sleuth Kit forensics tool to the mix. Among the other invitees, Network Associates and New Technologies Inc. (NTI) declined to participate, while iLook said it provides its software only to law enforcement. EMag Solutions, Forensic Explorer and Pictuality never responded to our invitation.

Each tool we tested will fill some investigative requirements. For example, Guidance Software's EnCase products are intuitive and address many aspects of a forensics inquiry. But EnCase Enterprise Edition is expensive and isn't all things to all organizations. That's where the other products in our roundup come in; each has strengths that will help you close the case. However, the contestants are too varied for an apples-to-apples comparison, so we divided the product reviews by three general investigation scenarios, or stages. Some categories will overlap, and, unless you require remote acquisition, the second-stage products should become your primary forensic-investigation tools.

Product Roll Call

- EnCase Enterprise
- ProDiscover
- Forensic
- EnCase
- Sleuth

• Stage 1: Network-capable initial analysis products for first responders, such as Guidance's EnCase Enterprise Edition and Technology Pathway's ProDiscover. These two products can acquire drive images remotely in a live environment, and their use eliminates the need for the Stage 2 tools.

• Stage 2: Primary analysis and drive-image acquisition. This stage usually entails obtaining the hard disk of a suspect machine and investigating it in a controlled (not live)

- dtSearch
- Paraben

Dig Deeper (on-site search queries)

- Network Forensics

Read On

- Network Forensics, Pt I
- RenewData Debuts Preservation Archiving Service
- Recovering From an Attack
- Reality IT: Prevention Is The Key To Network Security
- Body of Evidence

environment. AccessData Forensic Toolkit, Encase Forensic Edition and the open-source Sleuth Kit fit this stage. Any one can be used as the primary investigative tool in environments that don't require a network-capable acquisition application. All these products can acquire a full sector-by-sector drive image of any hard disk under investigation; additional sleuthing functionality varies by application.

• Stage 3: Fine-grained keyword searches through disk or partition contents, e-mail-specific searches or Internet history analysis. Paraben's NetAnalysis, E-Mail Examiner and Net E-Mail Examiner, and dtSearch's dtSearch excel here. These tools operate on disk images created by any of the applications from Stages 1 or 2.

Environmental Factors

Vendors at a Glance
Click to Enlarge

The applications you select will depend on your environment and the types of incidents you expect to deal with. It's a good idea to have a primary forensic tool that's supplemented with specialized applications. For example, text searches using the Stage 1 products EnCase Enterprise or ProDiscover failed to find text embedded in common formats, such as PowerPoint and Adobe PDF files. Fortunately, ProDiscover is relatively inexpensive, and even shops with small budgets could afford supplemental tools.

Obviously, if your company can afford all the bells and whistles of EnCase Enterprise, it should be on your shortlist. Guidance Software's combination of client state monitoring and network-capable forensic-image acquisition lives up to its everything-but-the-kitchen-sink reputation. But keep in mind that even the enterprise-network-capable products we looked at require other tools for a thorough investigation.

With remote functionality, a first responder can create an image of an affected system without having to shut down or transport the computer in question. Two of the products we tested can do this: EnCase Enterprise and ProDiscover. Of the two, EnCase Enterprise has the more polished interface, and the functionality to match, but, again, the cost may be prohibitive--$98,500 as tested. ProDiscover does just enough to be useful as a remote image-acquisition tool, without EnCase Enterprise's automated incident alert or advanced scripting functionality, and at $2,995, it's a fraction of EnCase Enterprise's price. Both tools claim to be able to remotely image any Windows file system, as well as Linux and Solaris file systems. Our tests included the remote acquisition of both FAT and NTFS Windows file systems.

If network drive preview and image acquisition aren't necessary, EnCase Forensic Edition or AccessData Forensic Toolkit can serve as your initial image-analysis tool. Supplement them based on your network configuration: Paraben's Network E-Mail Examiner, for example, is of no value in a Unix environment, but it's a necessity for Exchange users. If you are a Unix shop, Sleuth Kit is the answer.

Of course, even the best tool is useless if first responders and incident investigators aren't properly trained. In "CSI: Enterprise" (page 32), we outline steps for building an incident-investigation team with the expertise to secure your business and minimize risk--more important than any application.

◂ start top ▸ Introduction Stage 1: From a Distance ▸